



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/836,952	04/17/2001	Mehrban Jam	10005248-1	6956

7590 11/15/2007
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

EHICHIOYA, FRED I

ART UNIT	PAPER NUMBER
----------	--------------

2162

MAIL DATE	DELIVERY MODE
-----------	---------------

11/15/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 09/836,952	Applicant(s) JAM, MEHRBAN	
	Examiner Fred I. Ehichioya	Art Unit 2162	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1 - 38 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1 - 38 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This Office Action is responsive to communication filed September 4, 2007.
2. Claims 1 - 38 are pending in this Office Action.

Specification Objections

3. The amendment to specification overcomes the specification objections of last Office Action. Therefore the objection to the specification has been withdrawn.

Claim Rejections - 35 USC § 101

4. Amendment to the specification and claims overcome the rejection of claims 13 – 19 and 31 – 35 under 35 U.S.C. 101. Therefore the rejection of claims 13 – 19 and 31 – 35 under 35 U.S.C. 101 has been withdrawn.

Response to Arguments

5. Applicants argue:

(a) there is absolutely no teaching provided in § 4.2.8 of Ljungh of “identifying a lowest clearance level from among the clearance levels assigned to the smart badges within the boundary” (page 15, paragraph 4).

Examiner respectfully disagrees with the applicants. § 4.2.8 of Ljungh discusses both Guest badge and WIPS badge (smart badge). These badges are the same, perform the same functionality and could be assigned clearance levels. However, in § 4.2.8 of Ljungh, the lowest clearance level was identified for the Guest badge.

(b) there is absolutely no teaching provided in § 4.2.1 of Ljungh of providing access to that sub-set of information having clearance level no higher than the lowest identified clearance level (page 15, paragraph 6).

Examiner respectfully disagrees with the applicants. In § 4.2.1, Ljungh discusses providing different security levels to different doors within a building. Different security levels are sub-set of the whole security system. On page 6, Ljungh discloses information about which badge a person is wearing and the IP address of his laptop. The badge is assumed to have static IP addresses. Further on page 7, Ljungh discloses, "the database server has a method of finding out whether or not a particular user is allowed to see and update certain information in the database. These pages and section clearly suggests applicants claimed limitation "providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level"

(c) it is clear that Ljungh does not disclose the use of both IR and RF beacons for the purpose of detecting which smart badges are located within the predefined boundary (page 17, paragraph 2).

Examiner respectfully disagrees with the applicants. In § A.2, Ljungh discloses IR and RF that is placed as beacons inside a room and continuously transmit the room id information. Further paragraph 1 of page 17 (§ A.1) states "These beacons would emit a specific room id on a regular basis, which then could be detected by a smart device, a "badge", worn by the user. The badge would then transmit the information received through an Ethernet connection via an attached wireless LAN card to a central

Art Unit: 2162

server where the information would be processed and treated accordingly” The room id specifies the location of the smart badge.

6. In view of the above response to applicants’ argument, Examiner contends that the rejection of the last Office Action is proper.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1 – 38 are rejected under 35 U.S.C. 102(e) as being anticipated by Non-Patent Literature (NPL) “WIPS Technical Documentation by Roland Ljungh et al., (Hereinafter “Ljungh”).

Regarding claim 1, Ljungh disclose a computer-implemented method comprising:
assigning information stored on a computer a plurality of clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The

badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in order to have a particular entry through these doors);

using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level (see page 15, section 4.2.1 discusses providing different security levels to different doors within a building. Different security levels are sub-set of the whole security system. On page 6, Ljungh discloses information about which badge a person is wearing and the IP address of his laptop. The badge is assumed to have static IP addresses. Further on page 7, Ljungh discloses "the database server has a method of finding out whether or not a particular user is allowed to see and update certain information in the database. These pages and section clearly suggests applicants claimed limitation "providing access to that sub-set of the information having a clearance level no higher than the lowest identified clearance level").

Regarding claims 2 and 14, Ljungh discloses defining those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge); and updating the set of visible smart badges in response to a change in smart badge visibility status (see page 1, section 1, paragraph 2 wherein the badge server is updated when the person wearing the WIPS badge moves from one place to the other).

Regarding claims 3 and 15, Ljungh discloses recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 4, Ljungh discloses the method of claim 2 further comprising: recording the smart badge visibility status of each smart badge within an activity log (see page 10, section 3.3.1, paragraph 1 wherein the show room enables writing the name of specific room, badge/person wearing the badge when there is movement activities).

Regarding claims 5 and 16, Ljungh discloses providing access to smart badge wearers assigned to the smart badges (see page 15, section 4.2.1 wherein access is granted to badge wearer).

Art Unit: 2162

Regarding claims 6 and 17, Ljungh discloses the method of claim 2 further comprising:

preventing access to the information when the smart badge visibility status is set to invisible for a predetermined timeout (see page 9, paragraph 1 wherein access is denied when connection with the badge closes or timeout occurs).

Regarding claim 7, Ljungh discloses the method of claim 1 further comprising: writing data items to the smart badges (see page 9, paragraph 6 wherein commands are used to configure/ or write on the badge).

Regarding claim 8, Ljungh discloses the method of claim 7 further comprising: pre-reading the data items from the smart badges during idle periods (see page 9, paragraph 5 wherein data is read from the badge).

Regarding claims 9 and 18, Ljungh discloses defining a badge removal confidence level indicating whether each smart badge has been continuously worn by corresponding assigned smart badge wearers (see page 15, section 4.2.1 paragraph 1 wherein the badge is authenticated to verify that the badge is in the possession of the owner).

Regarding claims 10 and 19, Ljungh discloses assigning an expiration period to each of the smart badges (see page 9, paragraph 1 wherein the timeouts is interpreted as the expiration time); and

de-authenticating and erasing all data stored on a smart badge whose expiration period has been exceeded (see page 14, section 4.1.5 paragraph 2 wherein the administrator can edit or remove data from the badge).

Regarding claim 11, Ljungh discloses the method of claim 1 wherein the using element includes:

configuring the predefined boundary by varying a sensitivity level of the wireless beacon (see page 15, paragraph 1 wherein beacons are created according to the sensitivity level for example – light or dark sensitivity).

Regarding claim 12, Ljungh discloses a method for context-aware computer management comprising:

assigning database information a plurality of clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are

assigned access or clearance level in other to have a particular entry through these doors);

using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access);

defining those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge);

updating the set of visible smart badges in response to a change in smart badge visibility status (see page 1, section 1, paragraph 2 wherein the badge server is updated when the person wearing the WIPS badge moves from one place to the other); and

recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 13, Ljungh discloses a computer-usable medium embodying computer program code for context-aware computer management, comprising:

assigning database information a plurality of clearance levels (see page 13, section 4.1.2, paragraph 1 wherein “access levels” is interpreted as “clearance levels” and the administrator assigns or determines who is able to view which information);

assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in order to have a particular entry through these doors);

using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 20, Ljungh discloses a system for context-aware computer management comprising:

means for assigning database information a plurality of clearance levels(see page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as "clearance levels" and the administrator assigns or determines who is able to view which information);

means for assigning each smart badge within a set of smart badges one of the clearance levels (see page 15, section 4.2.1 wherein the doors are assigned security levels. The badge is associated with the door for authorizing access; inherently, badges are assigned access or clearance level in order to have a particular entry through these doors);

means for using a wireless beacon to detect which smart badges are located within a predefined boundary (see page 1, section 1, paragraph 2 wherein badges and location of the badges are identified using the IR beacons);

means for identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

means for providing access to that sub-set of the database information having a clearance level no higher than the lowest identified clearance level on a computer located within the predefined physical boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access);

means for defining those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge);

means for updating the set of visible smart badges in response to a change in smart badge visibility status (see page 1, section 1, paragraph 2 wherein the badge server is updated when the person wearing the WIPS badge moves from one place to the other); and

means for recalculating the lowest clearance level in response to the change in smart badge visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 21, Ljungh discloses a system for context-aware computer management comprising:

a database (see page 5, section 3.2.2), including information differentiated by a plurality of clearance levels (see page 13, section 4.1.2 wherein different access levels are disclosed);

a first wireless beacon (see page 1, section 1 paragraph 2 wherein the rooms are equipped with beacons which inherently include first and second beacons);

a set of smart badges, detected by the first wireless beacon to be within a predefined boundary (see page 1, section 1 paragraph 2 wherein the badge receives transmission from the beacon), each badge assigned one of the clearance levels (see

page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as "clearance levels");

computer located within the boundary (see page 16, section 4.2.5 wherein a portable computer is disclosed);

a system service module, coupled to the first wireless beacon (see Fig.1 wherein the beacon is connected to the badge/service module), for identifying a lowest clearance level assigned to the smart badges within the boundary (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

a software application, coupled to the system service module and the database, for providing access to that sub-set of the information within the database having a clearance level no higher than the lowest identified clearance level on the computer (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 22, Ljungh discloses the system of claim 21, wherein the first beacon includes: a wide angle RF beacon (see page 17, section A.2 wherein RF signal is placed as beacon).

Regarding claim 23, Ljungh discloses the system of claim 21, further comprising:
a second diffuse IR beacon, coupled to the service module, limited to detecting smart badges within the predefined boundary (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge).

Regarding claim 24, Ljungh discloses the system of claim 21, wherein the smart badges include:

biometric sensors for detecting when a smart badge has been removed from an assigned smart badge wearer (see page 15, section 4.2.1 wherein voice sensor is the biometric sensor).

Regarding claim 25, Ljungh discloses the system of claim 21, wherein the service module defines those smart badges within the boundary as a set of visible smart badges (see page 1, section 1, paragraph 2 wherein a person wearing WIPS badge is interpreted as visible smart badge), and

recalculates the lowest clearance level in response to a change in a visibility status (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 26, Ljungh discloses the system of claim 21, wherein the application logs smart badge wearers assigned to visible smart badges onto the computer (see page 10, section 3.3.1, paragraph 1 wherein the show room enables writing the name of specific room, badge/person wearing the badge when there is movement activities).

Regarding claim 27, Ljungh discloses the method of claim 1, wherein providing access to the sub-set of information comprises providing access to the sub-set of information stored on the computer located within the predefined boundary (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 28, Ljungh discloses the method of claim 1, wherein the wireless beacon comprises a first wireless beacon to communicate with the smart badges, the method further comprising:

using a second wireless beacon to communicate with the smart badges (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge),

wherein detecting which smart badges are located within the predefined boundary is based on the first and second wireless beacons (see page 9, paragraph 2 wherein a list of all beacons which inherently include first and second beacons are transmitted to the badge in order to detect which beacons are located in the room).

Regarding claim 29, Ljungh discloses the method of claim 28, wherein using the second wireless beacon comprises using the second wireless beacon to communicate with smart badges within the predefined boundary (page 17, paragraph 1 wherein beacons which inherently include first and second beacons communicate with the smart badges) and to communicate with smart badges outside the predefined boundary through one or more blocking objects defining the predefined boundary (see page 17, paragraph 6 wherein the signal are prone to travel through walls/outside boundary), and using the first wireless beacon comprises using the first wireless beacon to communicate with smart badges within the predefined boundary (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge), wherein the first wireless beacon is blocked from communicating with smart badges outside the predefined boundary by the one or more blocking objects (see page 17, paragraph 5 wherein the frequency signal is limited to limited area).

Regarding claim 30, Ljungh discloses the method of claim 29, wherein using the first wireless beacon comprises using an infrared beacon (see page 3 section 2.2), and wherein using the second wireless beacon comprises using a radio frequency beacon (see page 17, section A.2).

Regarding claim 31, Ljungh discloses an article comprising a computer-usable medium containing program code that when executed cause a computer to:

store plural sub-sets of information (see page 13, section 4.1.1), each sub-set of information associated with one of plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as "clearance levels" and the administrator assigns or determines who is able to view which information);

use at least a first wireless beacon to communicate with plural badges within a predefined region (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge), each of the plural badges associated with one of the plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as "clearance levels" and the administrator assigns or determines who is able to view which information);

determine a lowest clearance level from among the clearance levels associated with the badges in the predefined region (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

provide access to one or more sub-sets of the information having one or more respective clearance levels no higher than the determined lowest clearance level (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 32, Ljungh discloses the article of claim 31, wherein providing access to the one or more sub-sets of the information comprises displaying the one or more sub-sets (see page 10, section 3.3.1 wherein the functionality displays information about person, rooms and objects stored in the database) of the information having the

one or more respective clearance levels no higher than the determined lowest clearance level (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 33, Ljungh discloses the article of claim 31, wherein the program code when executed cause the computer to further:

use a second wireless beacon to communicate with the plural badges in the predefined region (page 17, paragraph 1 wherein beacons which inherently include first and second beacons communicate with the smart badges) and to communicate with one or more badges outside the predefined region (see page 17, paragraph 6 wherein the signal are prone to travel through walls/outside boundary),

wherein the first wireless beacon is able to communicate with the plural badges within the predefined region (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge) but is unable to communicate with the one or more badges outside the predefined region (see page 17, paragraph 5 wherein the frequency signal is limited to limited area); and

determining the badges that are within the predefined region based on the first and second wireless beacons (see page 9, paragraph 2 wherein a list of all beacons which inherently include first and second beacons are transmitted to the badge in order to detect which beacons are located in the room).

Regarding claim 34, Ljungh discloses the article of claim 31, wherein the program code when executed cause the computer to further:

receive a parameter from each of the badges, the parameter indicating a confidence level that the respective badge has been worn continuously by a user (see page 15, section 4.2.1 paragraph 1 wherein the badge is authenticated to verify that the badge is in the possession of the owner).

Regarding claim 35, Ljungh discloses the article of claim 31, wherein the program code when executed cause the computer to further:

re-determine the lowest clearance level as badges enter or leave the predefined region (see page 5, paragraph 1 wherein person events is generated when moved from one room to another in the re-access the security access level).

Regarding claim 36, Ljungh discloses a system comprising:

Storage (see page 5, section 3.2.2) to store sub-sets of information associated with corresponding plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as "clearance levels" and the administrator assigns or determines who is able to view which information);

a first wireless beacon to communicate wirelessly with badges within a predefined region (see page 1, section 1, paragraph 2 wherein IR beacon communicate with smart badge), each of the badges associated with one of the plural clearance levels (see page 13, section 4.1.2, paragraph 1 wherein "access levels" is interpreted as

Art Unit: 2162

“clearance levels” and the administrator assigns or determines who is able to view which information);

a module to identify a lowest clearance level from among the clearance levels of the badges within the predefined region (see page 16, section 4.2.8 wherein lowest priority levels regarding access is interpreted as lowest clearance levels); and

software to provide access to one or more sub-sets of information in the storage having one or more clearance levels no higher than the identified lowest clearance level (see page 15, section 4.2.1 wherein access is given in accordance different security levels. Different security levels are subset of the information or access).

Regarding claim 37, Ljungh discloses the system of claim 36, further comprising:

a second wireless beacon to communicate wirelessly with badges within the predefined region (page 17, paragraph 1 wherein beacons which inherently include first and second beacons communicate with the smart badges) and at least one badge outside the predefined region (see page 17, paragraph 6 wherein the signal are prone to travel through walls/outside boundary),

wherein the first wireless beacon is unable to communicate with the at least one badge outside the predefined region (see page 17, paragraph 5 wherein the frequency signal is limited to limited area),

the module to detect the badges that are within the predefined region based on the first and second wireless beacons (see page 9, paragraph 2 wherein a list of all

beacons which inherently include first and second beacons are transmitted to the badge in order to detect which beacons are located in the room).

Regarding claim 38, Ljungh discloses the system of claim 37, wherein the second wireless beacon comprises a radio frequency beacon (see page 17, section A.2), and the first wireless beacon comprises an infrared beacon (see page 3 section 2.2).

Conclusion

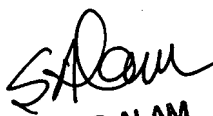
8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fred I. Ehichioya whose telephone number is 571-272-4034. The examiner can normally be reached on M - F 8:00 AM to 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John E. Breene can be reached on 571-272-4107. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


SHAHID ALAM
PRIMARY EXAMINER

/Fred I. Ehichioya/
November 9, 2007